

How to Fortinet

Local Out Route – FortiOS 7.0

Version 1.0





Inhaltsverzeichnis

EINFÜHRUNG.....	3
ALLGEMEIN ZUR KONFIGURATION.....	4
Interface Konfiguration:	4
Local Out Routing Möglichkeiten:	4
ANWENDUNGSBEISPIEL:	5
Konfiguration FortiAnalyzer Routing:	6
Konfiguration Routing System DNS	7
Konfiguration Routing zur FortiGuard	8
ERGEBNIS	9
FortiAnalyzer:	9
System DNS:	10
FortiGuard:	10

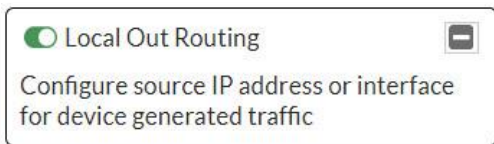
Einführung

Im FortiOS 7.0.0 ist ein neues Feature hinzugefügt worden, welches ermöglicht, verschiedene Local Out Services wie FortiAnalyzer, FortiGuard usw. über ein definiertes Interface zu routen. Diese Funktion ist sehr praktisch wenn mehrere ISP Interfaces oder noch spezielle ServiceLan's für bestimmte Dienste an die FortiGate angebunden sind. Das Feature Local Out Routing Feature unterstützt auch MultiVdom.

Feature aktivieren:

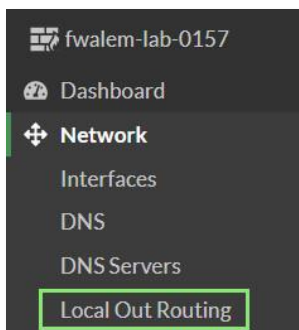
Damit man Local Out Routen im WebGui konfigurieren kann, muss zuerst das Feature aktiviert werden.

Über das Menu *System* → *Feature Visibility* in der Sektion Additional Features kann das *Local Out Routing* aktiviert werden



```
config system global
    set gui-local-out enable ← disable um das Feature zu deaktivieren
end
```

Jetzt erscheint unter dem Menu Punkt Network das Menu *Local Out Routing*:



Im Local Out Routing Konfigurationsfeld erscheinen jetzt die Services, welche von der FortiGate speziell geroutet werden können. Dabei sind ausgegraute Punkte nicht verfügbar, da sie in der jetzigen Konfiguration nicht verwendet werden. Zum Beispiel *Log syslogd Setting* wenn kein Syslog Server konfiguriert ist.

Name ↕	Source IP ↕	Outgoing Interface ↕
Log 4		
Log FortiAnalyzer Setting	198.18.0.157	service-lan (internal5)
Log FortiAnalyzer Cloud Setting	Dynamic	Auto
FortiGate Cloud Log Settings	Dynamic	Auto
Log Syslogd Setting	Dynamic	Auto
System 3		
System DNS	Dynamic	SD-WAN
System FortiGuard	Dynamic	Auto
System FortiSandbox	Dynamic	Auto

Allgemein zur Konfiguration


Was bedeuten die verschiedenen Optionen beim *Outgoing Interface*?

Outgoing interface ⓘ Auto SD-WAN Specify


Option	Beschreibung
Auto	Das ausgehende Interface wird automatisch anhand der Routing Tabelle definiert.
SD-WAN	Das ausgehende Interface wird automatisch anhand der SD-WAN Regeln definiert.
Specify	Das ausgehende Interface wird manuell definiert

Im Menu Punkt *Specify* habe ich die Möglichkeit Interface und IP-Adresse zu definieren: Dabei gibt es die Option, dass die Interface IP-Adresse benutzt wird oder dass man eine IP-Adresse auswählen welche z.B. als Sekundäre IP-Adresse auf dem Interface konfiguriert ist.

Interface Konfiguration:

Name  internal2

Alias

Type  Physical Interface

VRF ID ⓘ 0

Role ⓘ Undefined

Address

Addressing mode Manual DHCP Auto-man Interface IP PPoE

IP/Netmask

Secondary IP address ☒

+ Create New Edit Delete Q


IP/Netmask	Administrative access
10.157.1.1/255.255.255.0	Sekundäre IP Adresse

Auf dem Interface internal2 wird die IP-Adresse 10.157.0.1/24 Statisch (Manuel) vergeben. Hinzu wird noch eine Sekundäres IP-Netz 10.157.1.1/24 auf dem Internal2 Interface konfiguriert.

Local Out Routing Möglichkeiten:

Nun habe ich die Möglichkeit bei den Local Out Routen unter *Specify* die Source IP-Adressen auf *Manually* zu konfigurieren. Wenn ich das Interface internal2 auswähle, erscheinen mir die beiden IP-Adressen 10.157.0.1 und 10.157.1.1.

Outgoing interface ⓘ Auto SD-WAN Specify

 internal2

Source IP Use Interface IP Manually

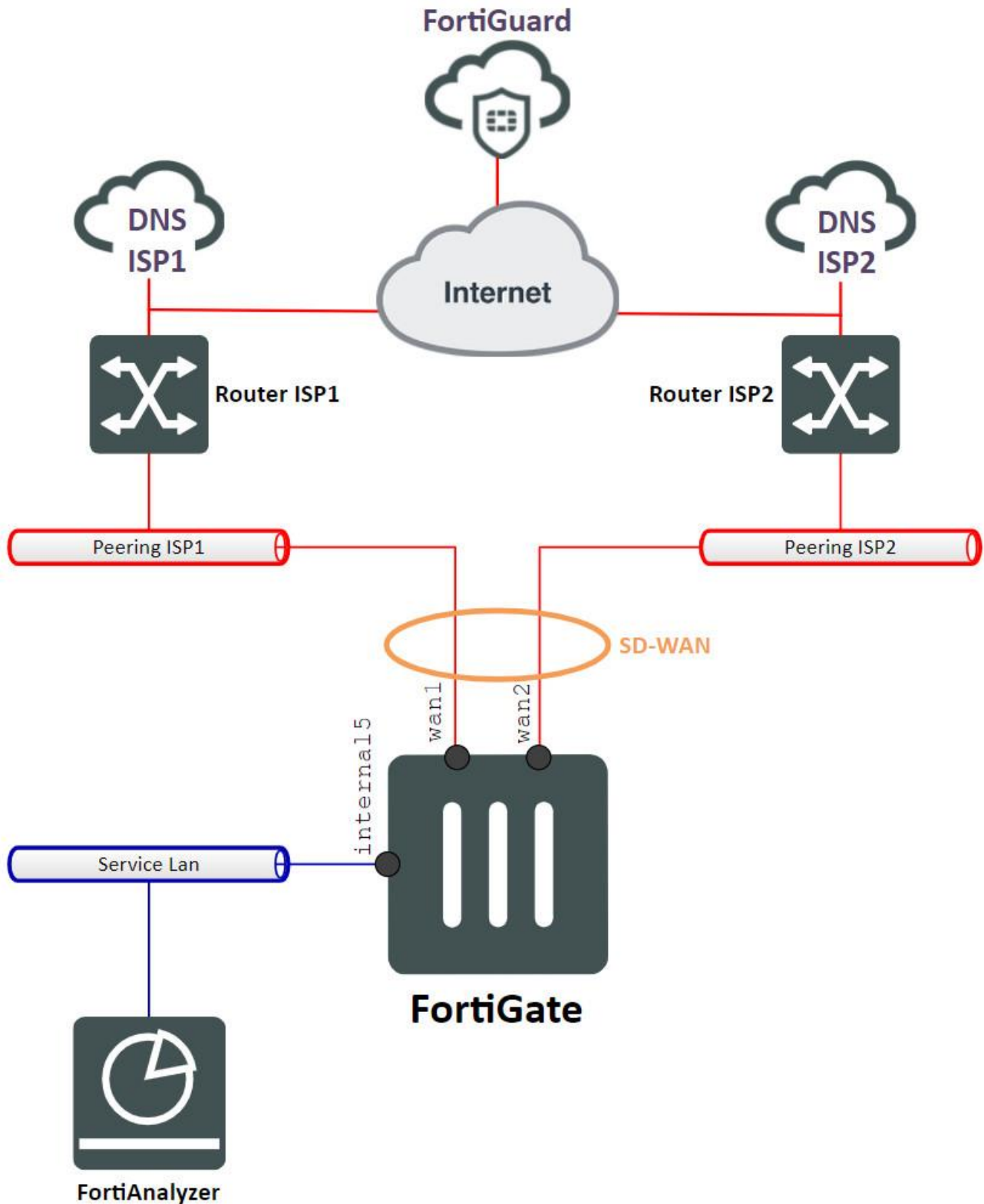
Interface IP

Sekundäre IP

Es können nur IP-Adressen ausgewählt werden, welche zum entsprechenden Interface einen Bezug haben.

Anwendungsbeispiel:

Mit folgendem Szenarium möchte ich das ganze ein wenig Fassbarer erklären:



Wir sehen in der Zeichnung das zwei ISPs an der FortiGate angeschlossen sind. ISP1 auf dem wan1 Interface und der ISP2 auf dem wan2 Interface. Dabei haben wir eine SD-WAN Zone mit dem wan1 und wan2 Interface gebildet.

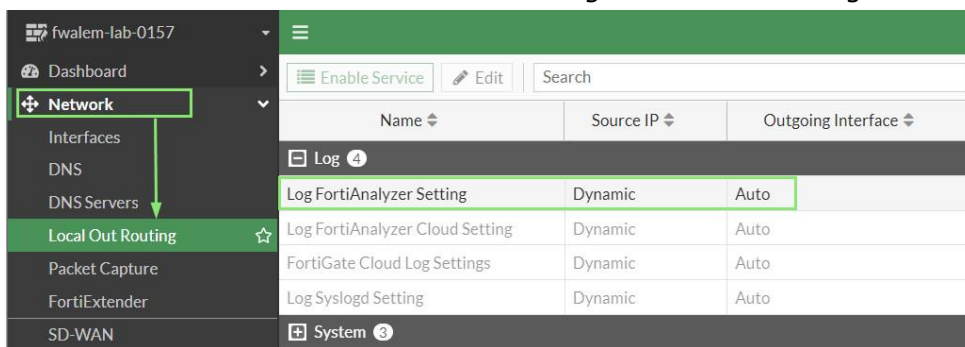
Der FortiAnalyzer ist über ein Service Lan an der FortiGate über das Interface internal5 angeschlossen und soll auch darüber mit der FortiGate kommunizieren.

Folgendes soll gewährleistet werden:

- Die FortiGuard soll automatisch das beste Interface wählen.
- Der System DNS wollen wir über beide SD-WAN Interfaces routen.
- Der FortiAnalyzer muss über das ServiceLan erreicht werden können.

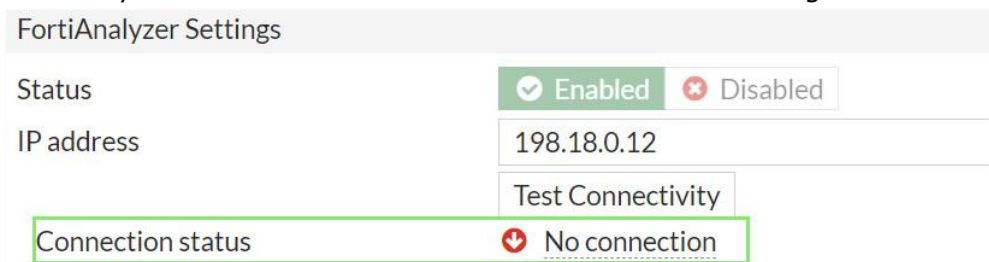
Konfiguration FortiAnalyzer Routing:

Über das Menu *Network* → *Local Out Routing* kann in das Konfiguration Menu gelangt werden.

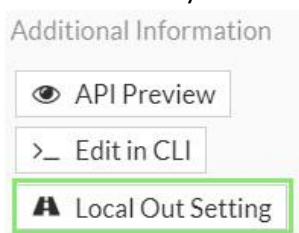


Wir sehen jetzt, dass der FortiAnalyzer Automatisch ein Interface und Dynamisch eine IP-Adresse wählt.

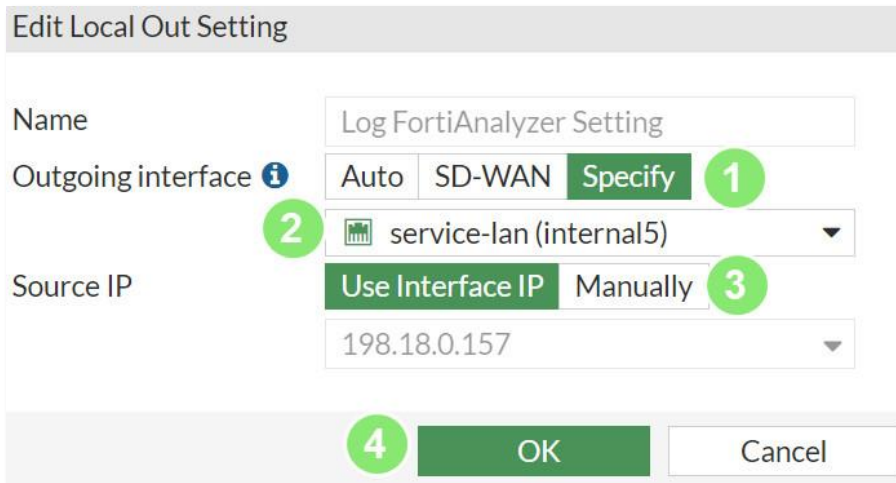
Dies kann dazu führen, dass die FortiGate über ein nicht vorgesehenes Interface versucht den FortiAnalyzer zu erreichen und wir dadurch einen Verbindungsfehler bekommen:



Wir werden jetzt die Local Out Route für den FortiAnalyzer konfigurieren: Dafür kann man direkt vom FortiAnalyzer Menu im Menu Punkt *Local Out Setting* gehen.



Natürlich kann auch über das klassische Local Out Routing Menu navigiert werden.

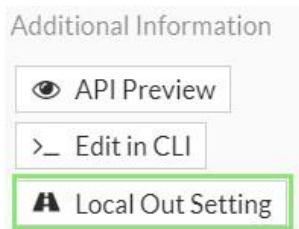


1. Ausgehendes Interface auf *Specify* setzen
2. Das service-lan (internal5) Interface auswählen
3. Die Interface IP-Adresse benutzen. Mit dieser IP-Adresse wird die FortiGate beim FortiAnalyzer wahrgenommen.
4. OK schliesst die Konfiguration ab

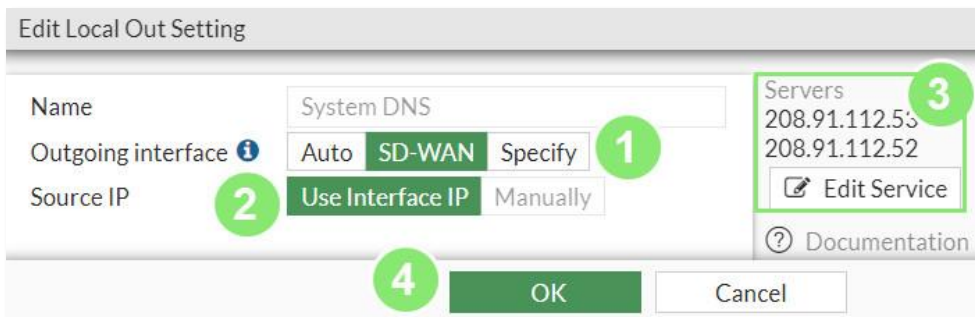
```
config log fortianalyzer setting
    set interface-select-method specify
    set interface "internal5"
    set source-ip "0.0.0.0"
end
```

Konfiguration Routing System DNS

Man kann auch hier direkt von der System DNS-Konfiguration im Menu Punkt *Local Out Setting* zu den Local Out Routings gelangen:



Oder man navigiert über den Local Out Routing Menupunkt in die Konfigurationsoberfläche:
Unter dem Abschnitt System der Punkt *System DNS* auswählen:

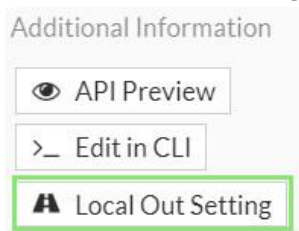


1. Ausgehendes Interface auf *SD-WAN* setzen
2. Bei Source IP wird die jeweilige Interface IP-Adresse verwendet Use Interface IP)
3. Wir sehen die konfigurierten System DNS-Server. Über Edit Service kann direkt in das System DNS-Menu gewechselt werden
4. Mit OK die Konfiguration abschliessen.

```
config system dns
    set interface-select-method sdwan
end
```

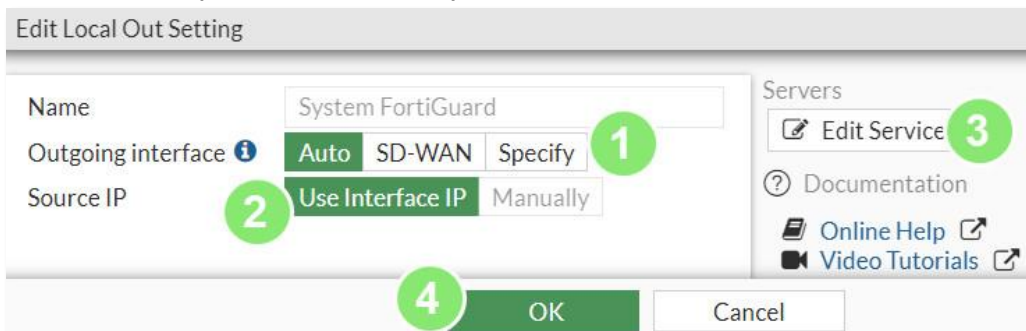
Konfiguration Routing zur FortiGuard

Vom FortiGuard Konfigurationsmenu kann auch direkt zu den Local Out Routen gelangt werden:



Alternativ über Local Out Routing navigieren:

Im Abschnitt System den Punkt *System FortiGuard* anwählen:



1. Ausgehendes Interface auf *Auto* setzen
2. Bei Source IP wird die jeweilige Interface IP-Adresse verwendet Use Interface IP)
3. Über Edit Service kann direkt in die FortiGuard Distribution Network Konfiguration navigiert werden.
4. Zum Bestätigen OK wählen.

```
config system fortiguard
    set interface-select-method auto
end
```


Ergebnis

Die Services werden jetzt wie gewollt geroutet:

Name ↕	Source IP ↕	Outgoing Interface ↕
Log 4		
Log FortiAnalyzer Setting	198.18.0.157	service-lan (internal5)
Log FortiAnalyzer Cloud Setting	Dynamic	Auto
FortiGate Cloud Log Settings	Dynamic	Auto
Log Syslogd Setting	Dynamic	Auto
System 3		
System DNS	Dynamic	SD-WAN
System FortiGuard	Dynamic	Auto
System FortiSandbox	Dynamic	Auto

FortiAnalyzer:

```

fwalem-lab-0157 # diag sys session filter dst 198.18.0.12
fwalem-lab-0157 # diag sys session list

session info: proto=6 proto state=01 duration=17991 expire=3595 timeout=3600 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=rsh vlan_cos=255/255
state=log local
statistic(bytes/packets/allow_err): org=413544/7199/1 reply=306665/3605/1 tuples=2
tx speed(Bps/kbps): 22/0 rx speed(Bps/kbps): 17/0
origin->sink: org out->post, reply pre->in dev=0->12/12->18 gwy=0.0.0.0/198.18.0.157
hook=out dir=org act=noop 198.18.0.157:8777->198.18.0.12:514 (0.0.0.0:0)
hook=in dir=reply act=noop 198.18.0.12:514->198.18.0.157:8777 (0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00006c0b tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu state=00000000
no_ofld_reason: local
fwalem-lab-0157 # diag sniffer packet any "host 198.18.0.12" 4
interfaces=[any]
filters=[host 198.18.0.12]
2.389952 internal5 out 198.18.0.157.8777 -> 198.18.0.12.514: psh 895497223 ack 2558983702
2.390352 internal5 in 198.18.0.12.514 -> 198.18.0.157.8777: psh 2558983702 ack 895497257
2.390426 internal5 out 198.18.0.157.8777 -> 198.18.0.12.514: ack 2558983745
4.109882 internal5 out 198.18.0.157.16255 -> 198.18.0.12.514: udp 477
5.249888 internal5 out 198.18.0.157.8778 -> 198.18.0.12.514: psh 3863284655 ack 4177359170
5.250222 internal5 in 198.18.0.12.514 -> 198.18.0.157.8778: psh 4177359170 ack 3863284689
5.250288 internal5 out 198.18.0.157.8778 -> 198.18.0.12.514: ack 4177359213
7.399907 internal5 out 198.18.0.157.8777 -> 198.18.0.12.514: psh 895497257 ack 2558983745
7.400319 internal5 in 198.18.0.12.514 -> 198.18.0.157.8777: psh 2558983745 ack 895497291
7.400389 internal5 out 198.18.0.157.8777 -> 198.18.0.12.514: ack 2558983788

```

System DNS:

```
fwalem-lab-0157 # diag sniffer packet any "port 53" 4
interfaces=[any]
filters=[port 53]
wan1 out 192.168.1.95.4181 -> 192.168.1.1.53: udp 27
wan1 in 192.168.1.1.53 -> 192.168.1.95.4181: udp 43
wan2 out 146.4.73.72.4181 -> 146.4.73.65.53: udp 35
wan2 in 146.4.73.65.53 -> 146.4.73.72.4181: udp 268

fwalem-lab-0157 # diag sys session filter dport 53
fwalem-lab-0157 # diag sys session list

session info: proto=17 proto_state=01 duration=70 expire=176 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=255/255
state=log local nds
statistic(bytes/packets/allow_err): org=120/2/1 reply=369/2/1 tuples=2
tx speed(Bps/kbps): 1/0 rx speed(Bps/kbps): 2/0
origin->sink: org out->post, reply pre->in dev=0->5/5->18 gwy=0.0.0.0/192.168.1.95
hook=out dir=org act=noop 192.168.1.95:4181->192.168.1.1:53(0.0.0.0:0)
hook=in dir=reply act=noop 192.168.1.1:53->192.168.1.95:4181(0.0.0.0:0)
misc=0 policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00009dd7 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=2 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
np_u_state=00000000
no_ofld_reason: local

session info: proto=17 proto_state=01 duration=62 expire=118 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=255/255
state=log local nds
statistic(bytes/packets/allow_err): org=71/1/1 reply=304/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org out->post, reply pre->in dev=0->6/6->18 gwy=0.0.0.0/0.0.0.0
hook=out dir=org act=noop 146.4.73.72:4181->146.4.73.65:53(0.0.0.0:0)
hook=in dir=reply act=noop 146.4.73.65:53->146.4.73.72:4181(0.0.0.0:0)
misc=0 policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00009ddd tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
np_u_state=00000000
no_ofld_reason: local
```

FortiGuard:

```
fwalem-lab-0157 # diag sniffer packet any "port 8888" 4
interfaces=[any]
filters=[port 8888]
57.766328 wan2 out 146.4.73.72.3748 -> 96.45.33.64.8888: udp 64
57.917133 wan2 in 96.45.33.64.8888 -> 146.4.73.72.3748: udp 12
57.955508 wan2 out 146.4.73.72.14927 -> 96.45.33.64.8888: udp 64
58.107836 wan2 in 96.45.33.64.8888 -> 146.4.73.72.14927: udp 12
174.549443 wan2 out 146.4.73.72.23987 -> 96.45.33.64.8888: udp 64
174.556676 wan2 out 146.4.73.72.14090 -> 96.45.33.64.8888: udp 64
174.699688 wan2 in 96.45.33.64.8888 -> 146.4.73.72.23987: udp 12
```